BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

PATENT
4001-1003

IN THE U.S. PATENT AND TRADEMARK OFFICE

In re application of: Mathias BISCHOFF et al.

Appl. No.: 10/036,401 Group: 2633

Filed: January 7, 2002 Examiner:

For: DEVICE AND METHOD FOR RESTORING CONNECTIONS IN AUTOMATICALLY SWITCHABLE OPTICAL NETWORKS

SUBMISSION OF ENGLISH TRANSLATION OF PRIOR PROVISIONAL APPLICATION UNDER 37 CFR §1.78(a)(5)

Assistant Commissioner for Patents

Washington, D.C. 20231

Sir:

In order to perfect applicants' claim for priority under 37 CFR §1.78(a)(5), applicants timely submit herewith an accurate English translation of prior provisional application No. 60/260,037, filed on 5 January 2001 in the German language.

Applicants wish to point out that a duplicate copy of the specification of the non-provisional application was inadvertently and erroneously identified as an accurate English translation of the prior provisional application in the Submission under CFR §1.78(a)(5) filed on January 7, 2002.

Respectfully submitted,

YOUNG & THOMPSON

By Benoît Castel

Benoît Castel
Attorney for Applicant
Registration No. 35,041
745 South 23rd Street
Arlington, VA 22202
Telephone: 703/521-2297

April 30, 2002

VERIFICATION OF TRANSLATION

I, Joe Crabbs, a translator with Chillson Translating Service, 3530 Chas Drive, Hampstead, Maryland, 21074, hereby declare as follows:

That I am familiar with the German and English languages;

That I am capable of translating from German to English;

That the translation attached hereto is a true and accurate translation of German U.S. provisional 60/260,037 titled, "Restoration of links in automatically switched optical networks (ASON);"

That all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true;

And further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any registration resulting therefrom.

By Joseph Crabbs

Executed this 30 day of April 2002.

Witness Anne Allen

Title: Restoration of links in automatically switched optical networks (ASON)

Continue with the mouse or bottom arrow key (Brief instructions for answering the following questions can be found in HL Intranet/MchB/Patents/Readme)

1. What technical problem is the invention supposed to solve?

2. How was this problem solved in the past?

3. How does your invention solve the indicated technical problems (indicate advantages)?

4. Wherein does the inventive step lie?

5. Embodiment(s) of the invention

Begin below this line with statements for item 1 to 5

1.) In a future transport network (automatically switched optical network ASON), in addition to the classical method of "protection switching" (alternate circuit with prior reservation of an alternate connection) for protecting connections against failures of links, nodes or other parts of the network, the dynamic method of "restoration" which conserve resources will also be used. Here alternate paths are sought only after failure of a link or the like for the affected connections. The question arises which network node is responsible for restoration of a connection so that the connection is set up again as quickly as

possible and with local knowledge. This question is answered in this application.

2.) In classical transport networks restoration is not offered, but connections are protected by alternate connections to which it is possible to quickly switch with the alternate circuit process. For ASONs there are proposals [1] for assigning the task of restoration to the source node of the connection which is already looking for two disjoint paths [2] through the network when a connection is set up and thus, without looking for other routes when a user connection fails, immediately knows an alternate route which is not affected by this failure and to which the alternate connection can be switched.

3.) Assuming that the routing in ASON is carried out with a "link state" algorithm [3], after receiving a message about a configuration change each network node immediately knows the new network topology and can thus determine the new shortest path free of loops to the destination of a connection which has been interrupted by failure. This task can fundamentally be easily transferred to the source node of the connection (that node from which the connection was originally set up), as is shown in Figures 1-3. Figure 1 shows one example for a transport network with 10 network nodes A-H and 16 links between them which each are supposed to have a distance metric of 1. A connection between nodes A and F is set up and confirmed according to the flow chart shown in Figure 3, part 1, along route A-B-C-D-E-F. After failure of the link between D and E the network appears as is shown in Figure 2. This link failure is signalled by the two

nodes D and E each to all neighboring nodes (part of the routing protocol, not shown) in the form of flooding so that all other network nodes are notified as quickly as possible about this change of topology. Afterwards nodes D and E for each now interrupted connection send a message with which the responsibility for restoration of the connection is explained. This message is sent along the original connection path. In Figure 3 node A is supposed to be responsible for restoration as the node which had originally set up the user connection. Therefore node F receives from E the message N_RELEASE (connection release after network fault without responsibility for restoration). Conversely, node D sends in the direction to the source of the connection the message N_RELEASE_RECONN (connection release after network fault with responsibility for restoration). It is routed along the original connection path from D via C to B and from the latter further to the source node A which thereupon sets up a new connection to F via nodes K-J-H-G.

The case shown in Figure 3 corresponds to delegation of responsibility for restoration to the source node of the connection. Especially for very prompt restoration, it can be advantageous on the other hand if a connection is re-routed nearer the fault site with acceptance of a possibly somewhat longer path. It is proposed as claimed in the invention here that the return of responsibility for reestablishing the connection is pursued only until

1) an alternative path to the destination is found and

2) the distance metric to the destination has no longer been reduced one step long (the additional step naturally having to be considered) or

3) responsibility has reached the starting node of the connection.

For this reason a parameter is also given to N_RELEASE_RECONN messages (NRR) which states how great the distance is from the node transmitting the message to the destination. If the aforementioned conditions are met, the message is no longer forwarded to a predecessor node, but the alternate connection is set up.

Figure 4 will be used for purposes of description. After the information about topology changes in the network has been flooded (Figure 4, part 2), nodes D and E first transmit the N_RELEASE and N_RELEASE_RECONN messages (Figure 4, part 3). Message NRR(4) from node D to node C notifies the latter that node D could set up an alternate connection with metric 4 (sum of link metrics computed from D), the length of the entire path from A via D to F would therefore be 7. C itself however has only one path of length 3 (total path length 5) and delivers this in turn to node B. B itself would again need 4 steps (total path length 5), would therefore choose the same path via C as C itself. Therefore B does not relay the message to A, but itself sets up the alternate connection to H (Figure 4, part 4).

This example shows how the indicated algorithm ("look for new path and set up connection as soon as the new path ceases to become shorter) achieves the establishment of an alternate

connection relatively near the failure site, but without unnecessary double paths. Each node must compare only the distance metric received in the N_RELEASE_RECONN (NRR) message with its own new distance to the connection destination so that ultimately a local decision for the alternate route and for the responsibility for setting up the alternate connection is possible. It is also possible that using this algorithm the globally optimum solution is not found; this can also be duplicated only in larger network examples.

Options and expansions

1. In contrast to the description above and in the figures, the responsibility for setting up an alternate connection from the fault site is not given in the direction of the node which originally set up the connection, but in the opposite direction (destination of the original connection set-up) or this responsibility is fixed according to another globally unambiguous metric (for example, those end nodes with the numerically smaller and larger network address).

2. Error-protected or non-error-protected transmission of the messages shown in Figures 3 and 4.

3. Combination of flooding messages with a list of service connection endpoint identifiers to be re-established/affected by the failure.

4. Additional limitation of back path length n_{Back} so that at latest after n_{Back} steps of the algorithm, establishment of the alternate condition is started.

5. Exclusive use of the back path length n_{Back} as the criterion without examining the distance metric. The example in Figure 4 would randomly correspond to the case $n_{Back} = 2$. Setting up the alternative connection basically by one of the end nodes of the failed link would correspond to $n_{Back} = 0$ and set-up basically by the starting node of the connection would correspond to n_{Back} = infinity.

6. A node which receives a N_RELEASE_RECONN message decides with a Bernouilli experiment (for example, via a pseudorandom number generator) randomly whether it is responsible for restoring the connection, or whether it relays the N_RELEASE_RECONN message to the next predecessor node on the original connection path. The probability of one decision or the other can thus be stipulated differently per node or uniformly network-wide.

7. Determination of the probabilities for option 6 node by node using the number of links connected to the node.

8. Determination of the probabilities for option 6 case by case using the distance (routing metric) to the source node of the connection.

9. Determination of the probabilities for option 6 case by case using the distance (routing metric) to the destination node of the connection.

10. Determination of the probabilities for option 6 node by node using the instantaneous usage of the links connected to the node.

11. If the node which finally sets up the alternate connection routes it first along the path of the old connection, it can instruct the next node to continue to use the corresponding fragment of the old connection. In Figure 4, B would not send a connection set-up message to C, but would send a modified RECONNECT message.

12. The decision, from what side of the failed link the connection is to be re-established (see description and option 1) can be made depending on the distance between the failure site and the end nodes of the connection. To do this, when the user connection is set up for the first time each participating node must enter into its connection table the lengths of the routes to the two end nodes. When a link or node fails then each of the two affected edge nodes of the failure area compares these two values, taking into account that the node on the other side of the failure area has entered a path shorter than in the link table by the failure path segment. In the case in which these distance metrics are the same for both sides the responsibility is explained according to the original description or according to one of the possibilities in option 1.

13. Like option 12, however all nodes enter the side responsible for restoration in the case of a link failure when the connection is set up. This however can lead to inconsistences when a larger component network fails.

4.) Algorithm for optimum establishment of the responsibility for restoration of an interrupted connection in ASONs with restoration.

5.) ASON network node which contains the algorithm and communicates accordingly with its neighbors

Bibliography

[1] Siemens IP over WDM ASON Architecture Specification, July 2000

[2] J.W. Suurballe, "Disjoint Paths in a Network", Networks Vol. 4, 1974, pp. 125-145

[3] Christian Hulterna, Routing in the Internet, Prentice-Hall, 1996, ISBN, 3-8272-9526-2, pp. 118-126

Continue with mouse or right arrow key

6. The following are enclosed as attachments for further explanation:

1 page of the description of one or more embodiments of the invention; (if possible prepare drawings in PowerPoint or Designer format)

30 pages of literature which describes the prior art underlying the invention*)

*) Please attach photocopies or offprints of all cited publications (articles complete; for books the relevant chapters with complete bibliographic data.

7. Which agencies are interested in the invention? ICN TR

8. Has the invention already been tested (completion of tests, preparation of models) no

9. For what products can be invention be used? network nodes for OTN/ASON, SDH

10. Is the application of the invention provided? no

11. Has a product based on the invention been delivered or is a delivery intended? no

12. Is publication of the invention intended or has it already taken place? no

13. Is communication of the invention to those outside of the company intended or has this already taken place? yes

(presumably) on 8/25/2000 to D. Schupke, TU Munich (co-inventor)

If possible, please assess the following criteria:

a Difficulty for competitors to circumvent

Equivalent alternatives

require effort

b Attractiveness to competitors for use

average

c. Evidence of competitor use

Evidence of use

easily possible

d. Use in house

unresolved

Figure 1: Example of a transport network with 10 nodes A-K. All links are supposed to have a distance metric of 1

Figure 2: Network from Figure 1 after failure of link D-E

Figure 3: Flowchart for Figure 1/2

1. Connection set-up between clients on nodes A and f

2. Link failure D-E and flooding of this information to all network nodes

3. Delegation of restoration from D to C to B to A

4. Restoration by node A via alternate path

Within Figure

2 Link failure: Link D-E no longer usable starting now

Below Figure:

Connection set-up (SETUP)

Confirmation for connection set-up (SETUP_OK)

Connection release after network fault with restoration stipulation (N_RELEASE_RECONN)

Connection release after network fault without restoration stipulation (N_RELEASE)

Figure 4: Flow chart with the proposed algorithm

1. Connection set-up between clients on nodes A and H

2. Link failure E-F and flooding of this information to all network nodes

3. Delegation of restoration from D to C and from C to B; release of connection between E and F

4. Restoration by node B

Within Figure

2 Link failure: Link D-E no longer usable starting now

Below Figure:

Connection set-up (SETUP)

Confirmation for connection set-up (SETUP_OK)

Connection release after network fault with restoration stipulation (N_RELEASE_RECONN)

Connection release after network fault without restoration stipulation (N_RELEASE)

SIEMENS

ASON Architecture Specification

Issued by
ICN
Hofmannstraße 51, D-81359 München

SIEMENS AKTIENGESELLSCHAFT

Editor: Pauluhn

ICN TR ON DT 5

In addition to the editor named on the cover page the following persons have collaborated on this document:

Dr. M. Bischoff	ICN TR ON DT 5
Dr. J. Charzinski	ICN M NT 19
B. Stilling	ICN TR ON DT 5
D. Schupke	Munich University of Technology, Institute of Communication Networks,

This document comprises 27 pages, all of them are in Issue v1.0

This document is based on the template \\MCHH285A\FS001245\PowerWDM\Specs\pwdm_template.dot

This issue was last modified on 19.07.2000 17:38.

This document was edited with MS Word Version 97.

This document is stored under the file name ASON Architecture Specification.doc.

TABLE OF CONTENTS

0 GENERAL INFORMATION

0.1 Issue Control

This document comprises 27 pages, all of them are in issue v1.0.

0.2 History

Issue	Date	Reasons for Change
v1.0	19.07.00	1st version reviewed by authors

Table 0-1: History

0.3 References

[1] T1X1, January 2000: Further Discussion of Requirements for Automatically Switched Optical Channel Networks, Nortel
[2] ODSI Framework
[3] draft-ietf-mpls-cr-ldp-03.txt, Oct. 99
[4] draft-ietf-mpls-ldp-06.txt, Oct. 99
[5] ITU-T SG13 TD 44 (WP3/13): First Draft of Rec. G.ason, "Architecture for the Automatic Switched Optical Network" (ASON), Kyoto, Japan, Feb./Mar. 2000
[6] S. Chaudhuri et al: "Control of Lightpaths in an Optical Network", OIF Contribution
[7] ITU-T: Recommendation G.805, "Generic functional architecture of transport networks", Geneva, 1995.
[8] Huitema: "Routing in the Internet", Prentice Hall, 2000

0.4 List of Abbreviations

ASON	Automatically Switched Optical Network
ATM	Asynchronous Transfer Mode
IETF	Internet Engineering Task Force
IP	Internet Protocol
IS-IS	Intermediate System to Intermediate System (Protocol)
NARP	NBMA Address Resolution Protocol
NBMA	Non-Broadcast, Multi-Access
NHRP	Next Hop Resolution Protocol
NNI	Network Node Interface
OCh	Optical Channel
ODSI	Optical Domain Service Interconnect
OSC	Optical Supervisory Channel
OSPF	Open Shortest Path First
RI	Registry Interface
SDH	Synchronous Digital Hierarchy
STM	Synchronous Transport Module

TDM	Time Division Multiplex
UNI	User Network Interface
WDM	Wavelength Division Multiplex

0.5 List of Figures

0.6 List of Tables

1 INTRODUCTION

1.1 Scope of the Document

This document describes the architecture and essential functions of an automatically switched optical network in a rather abstract way, defining the required functional entities and the interactions between them. It does neither discuss the benefits of ASONs nor provide input for a respective business plan, but assumes that there is a demand for such networks and that this demand can be satisfied in an economical manner.

1.2 Outstanding Issues

The following items are not treated in this document, even though desirable for a complete picture:

- Security: includes authentication and authorization of the network client as well as the integrity and confidentiality of control information in the network in general
- Accounting management
- Network Management: important tasks of the TMN such as switching connections are now performed automatically which will affect the network management system.
- Interworking of ASONs: any additional requirements for the gateway nodes of ASON interworking

1.3 Document Overview

The document is organized as follows: Section 2 describes some general architectural assumptions this specification is based on. In Section 3 a Plane Model for ASONs is presented. Section 4 deals with the address requirements for the different network interfaces. Section 5 gives an overview of an ASON's functional entities and describes these entities, whereas Section 6 primarily shows the information flows between them for various events. It also describes in how to route a path through a hierarchically layered network.

2 GENERAL ASSUMPTIONS

At the time being, there is no common understanding within the I&C community what an ASON exactly looks like, e.g., which services it provides, which features operators require, or, what the relation to other networks is. However, the development of an architecture for an ASON is not possible without having some of the main questions answered, even if only a rough picture is drawn. The following sections describe the general assumptions on which the architecture of this specification is based. They reflect the opinion of the authors with respect to the likelihood of possible answers.

2.1 ASON Services

The service provided by the ASON is a circuit switched point-to-point connectivity service. The ASON is not able to handle data packets individually, or even to recognize that a connection is used to transport packets. All packet switching is considered to take place at the client layer.

The ASON connections are always bi-directional and symmetrical with respect to capacity. The two trails constituting a connection are always routed along the same route.

The establishment of a connection within the ASON may be triggered by a client via a UNI (switched connection, or a "call"), or may be triggered manually via the network management (soft permanent connection). The same is true for the release of a connection, of course. Despite its name, the term UNI in the context of this paper does not refer to an end user interface but to the interface between the ASON and its client network nodes like switches and routers.

In principle the ASON is client agnostic, serving all types of clients. In practice there are some constraints due to physical transmission impairments. It is therefore assumed, that analogue client signals, which are most sensitive to signal distortions, are not supported by the ASON. The clients of the ASON are digital network nodes offering digital signals with known physical layer characteristics at their interfaces. Because only clients with interfaces of the same type can be connected, the ASON has to know the signal type of each of its clients. It is assumed, that there is a well defined set of supported client signals comprising at least SDH (STM-16, STM-64, STM-256) as well as Gigabit Ethernet and the future 10 Gigabit Ethernet. Also a transparent optical channel service and an optical band service (fiber bandlimited by optical amplifiers) may be offered. It should be noted, that the ASON, despite it is discussed mainly in the context of IP transport, supports also non-IP clients.

The ASON supports a number of service classes differing with respect to the connection availability. The availability is a function of connection priority (low priority traffic may be bumped to get resources needed for high priority traffic) and of failure survivability. Failure recovery mechanisms are divided into protection and restoration mechanisms. In case of protection the back-up resources are reserved at the time the working connection is established. In case of restoration the back-up resources are allocated once a failure is detected, i.e. the back-up path is dynamically established at the time it is required using network wide spare resources. If no back-up path can be found the connection is lost.

Protection mechanisms rely on dedicated switching gear being part of the data plane without interfering with the control plane. Hence, they are out of the scope of an ASON. However, the ASON must support establishing back-up paths (protection connections) which are diversely routed to the respective working paths. Diversity can mean link diversity or node diversity, where link diversity comes in different flavors (fiber diversity, cable diversity, duct diversity). To assure this, shared risk groups will be used, providing the routing algorithm with the relevant information. Also the ASON may support routing preferably over protected links.

Service classes can further be differentiated using two types of connections. The two types differ with respect to their "stiffness". Stiff connections, once established, remain as they are until they are released. In contrast, flexible connections may be rerouted during service to allow for network optimization. The attribute of stiffness holds on an end-to-end basis, i.e., the subnetwork connections forming a connection are either all stiff or all flexible. A mix of stiff and flexible subnetwork connections is not supported. Using the two connection types, different service grades with respect to survivability can be constructed, see Table 2-1.

Service Grade	Working Connection	Back-up Connection	Remark
1	Stiff	Stiff	
2	Stiff	Flexible	
3	Flexible	Stiff	Does not make much sense.
4	Flexible	Flexible	
5	Stiff	None	Is only affected by a failure along its trail.
6	Flexible	None	May also be affected by a failure in the vicinity of its trail.

Table 2-1: ASON survivability grades

(Note: By means of restoration further service grades can be constructed.)

2.2 Architecture Model

The ASON is a network offering its services to other networks. Hence, the question arises how the interworking between the ASON and its clients is managed. In the IP community this question is discussed on the basis of four architecture models originating from the discussion about the interworking between IP and ATM networks. Omitting details, there are essentially two approaches: one approach where the topology of the server network is hidden to the client network, the so-called overlay model, and another approach where the topology of the server network is known by the client network (integrated, augmented and peer model). In the latter case the topology information is exchanged explicitly between client and server, or the routing protocol does not differ between nodes of the client and the server network.

For an ASON supporting only IP clients an integrated or similar model seems to be appropriate. For an ASON supporting a lot of different clients this approach is at least questionable. Moreover, if we assume that the operator of the ASON and the operator of the client network is not identical, the exchange of complete topology information will be most probably not accepted. Therefore, we assume an overlay model. This means that the client network sees the ASON as a simple point-to-point link. The routing and signaling of the client and the server network is completely independent of each other, also if the same protocols are used. This model fits well with the services described above, e.g., there are also soft permanent connections provided through network management.

The overlay model has the drawback that client nodes after running their routing protocol do not know which connections the server network can provide and which not. In other words, a client node does not know if it can reach another client node via a connection to be provided by the server network or not. If all client nodes would be connected to the server network a demanded connection could only be rejected due to blocking in the server network or at the called node (all interfaces busy). In this case a trial-and-error approach would be sufficient. However, in general not all client nodes have a connection to the server network. In this case an explicit solution for the reachability problem has to be provided.

2.3 Multiplexing Hierarchy

The ASON is heterogeneous concerning the link transmission capacity. The links connecting the ASON nodes may differ with respect to the maximum number of OCh they can carry as well

as the bit rate per OCh. There may be transparent links and links fixed to a special payload type (e.g., STM-16) due to TDM employed on top of WDM. The TDM is used to maximize the transmission capacity per OCh while still keeping an acceptable granularity. If the signals at the end of a link are not always demultiplexed down to the originally client format but switched by the switching fabric as a bundle, this has serious consequences with respect to the network architecture: The ASON is split into several layer networks. This is true also when the switching matrices within the nodes are transparent and simultaneously switch connections of different bandwidth. Virtually they are separated into matrices for each switched signal type, whereby each virtual matrix belongs to the respective layer network, see Figure 2-1.

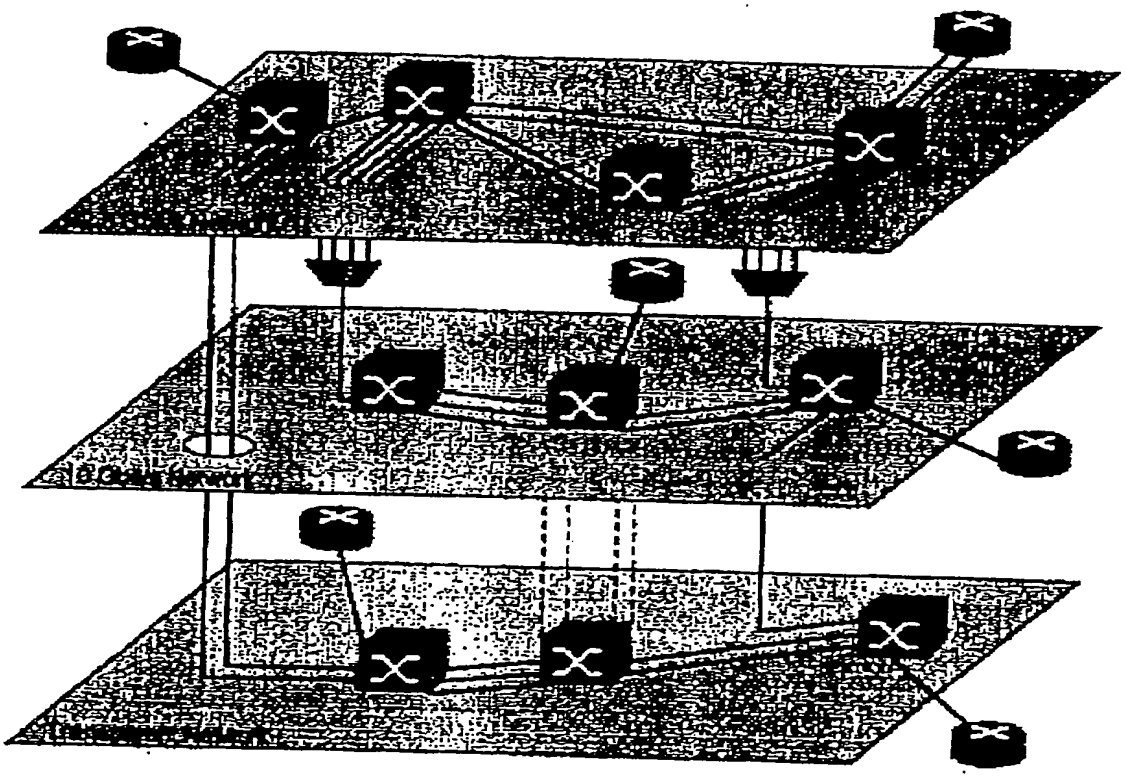

Figure 2-1: ASON split into several layer networks by TDM

The most important signal types will have their own ASON layers, which are effectively own logical networks optimized for the transport of the corresponding client signals. All signals without a dedicated layer network have to be transported in the transparent layer network. Also signals with a dedicated layer are not excluded to use the service of the transparent layer network, see Figure 2-1 . The different layer networks may share the same physical resources, of course. For instance, one part of the OChs of a link may be terminated on both sides with a TDM while the rest is connected transparently to the switching fabric. In this case the two layer networks share the same fiber and the same optical amplifiers.

2.4 Node Capabilities

It is assumed that in general an ASON node has an optical and hence transparent switching matrix. However, nodes which completely belong to one of the dedicated layer networks described above may employ an opaque matrix. Independently of implementation details it is assumed that only the client signal as a whole is switched and the node does not support switching of a fraction of the signal bandwidth. The node is not only blind with respect to individual packets but also with respect to individual time slots. The handling of both is assigned to the client layer networks.

Wavelength converters may also be transparent or opaque. Nodes may employ wavelength converters, or may not. In general, the wavelength constraint have to be taken into account during the routing process.

ASON nodes detect automatically the topology of the network they are connected to. This holds for initial equipment deployment as well as for topology changes due to failures. Client nodes attached to the ASON via an UNI register themselves in the network. This will happen also after a reboot of a failed client node. Client nodes without an UNI have to be registered manually.

3 ASON PLANE MODEL

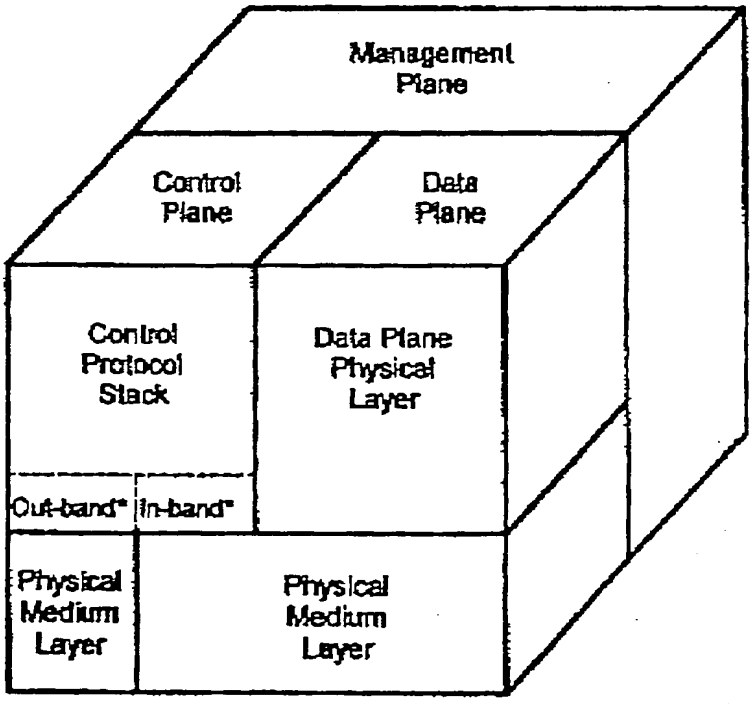

Figure 3-1: ASON plane model

*) If the control plane and the data plane share the same physical medium this is called an in-band control channel. An in-band control channel is directly related to the device's data port (facility associated) and enables service and topology auto-detection. If both planes use their own physical medium this is called an out-band control channel. In

this case the data plane and control plane are not physically coupled and auto-detection is problematic because the assignment between control and data plane is not physically guaranteed.

The ASON consists of three planes, the data plane, the control plane and the management plane. The data plane is responsible for circuit-switching data signals through the network, as well as for sourcing and sinking the data signals. The data plane consists of two layers, the data plane physical layer and the physical medium layer. The data plane physical layer performs the functions necessary for transmitting the user data over the physical medium. SDH over WDM could be a data plane physical layer protocol in an ASON. The physical medium layer provides the medium for transmitting the user data. The physical medium in an ASON is a fiber. The control plane runs routing and signaling protocols and is responsible for overall system operation. It is composed of a protocol stack performing the functions necessary to communicate to other instances and a physical medium layer providing the transport medium. Depending on the physical allocation of the control channel, in-band or out-band, the control plane and the data plane share the same physical medium or not, respectively. The management plane allows system operators to configure and monitor the network. The management plane is outside the scope of this document.

4 ADDRESSING

In a network offering automatic (signaled) path set-up, it is necessary to be able to address several service access points. Routing and signaling protocols run between network nodes, which should be addressed appropriately. Client signaling is possible over the UNI. Here an address is required both for the client signaling channel endpoint at the UNI as well as for the target remote connection endpoint. Also, for signaling inside the network, the physical resources between which a connection is to be established must have addresses. In addition, network and client nodes must be able to address the registry server(s) somewhere in the network.
In Figure 4-1, the addressing relations for user and control plane addresses are sketched, neglecting the registry servers at this point. There are different addresses required at the different reference points. For data channels at the NNI (A), both sides' addresses must provide a node, port, wavelength and channel identifier. Reference point (A) addresses will also be the ones transported in the payload of signaling and routing protocol messages. Signaling and routing messages at the NNI (B, C) must be able to address the corresponding partner entity. This can either be done by using the same node identifier as with (A) plus a signaling / routing protocol instance identifier or by using addresses belonging to a client network which is used for transporting signaling and routing messages. This choice can in principle be performed independently for reference point (B) and (C) addresses but in practice it is advisable to let both have the same kind of address. The UNI addressing options for data (D) and signaling (E) depend on the choice of network connectivity. If each interface is connected by a single-channel, single-wavelength point-to-point link, addressing can be implicit and no explicit addresses need to be used. However, most message based signaling protocols will require the partner instances to have addresses at reference points (E). For these, the same options as above (B,C) are possible: Addresses can be either specific optical network addresses (node id) or belong to a client network.

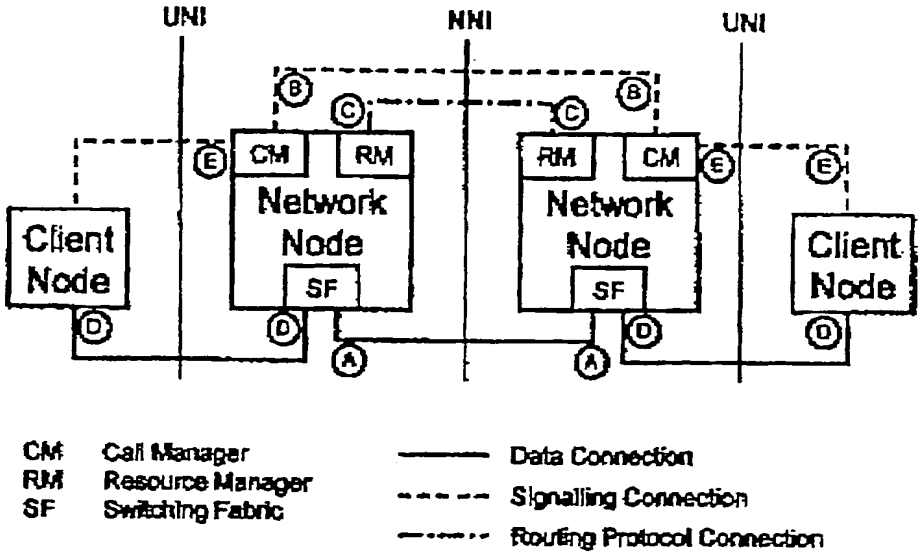

Figure 4-1: Addressing at different network interfaces

Another open point is the question of the addresses' scope. The addresses could have local or global significance. Making the addresses globally significant could make it easier for an optical transport network to provide global connectivity and cross-provider connection establishment.

As the Internet Protocol (IP) offers a world-wide connectivity of layer 3 instances, both ODSI and IETF have proposed to use IP addresses as node identifiers for optical networks [1-4]. This approach is justified if the major client layer for optical transport networks is going to be IP and if the control plane will be IP based. In this case, every node contains an IP instance anyway for handling the signaling and routing protocol messages, so that this IP address could be re-used on layer 1 as a node identifier. On the other hand, it might be advisable not to use IP addresses to identify optical network nodes if the addressed targets do not provide real IP instances (e.g. single ports of an optical network node, as suggested in [3]). Correspondingly, a current ITU draft [5] calls for these addresses to be disjoint from upper layer addresses, very much like Ethernet addresses are disjoint from IP addresses if transmission and client layer are properly separated.
We suggest to use IP addresses for signaling and routing entities (B, C, E reference points) and introduce special optical transport network addresses for the data channels (A and D reference points).

5 ASON FUNCTIONAL ENTITIES

5.1 Overview

The block diagram in Figure 5-1 shows the functional entities of an ASON. Three different nodes are distinguished: edge node, transit node and client node. An edge node is connected to a transit node or to an other edge node via the network node interface (NNI). Edge and transit nodes consist of a call manager, a resource manager, a switching manager, a link watcher and the physical resources. A client node is connected to an edge node via the user-network

Interface (UNI) and consists of a call manager and a service resolver. An address information service is provided by a registry.

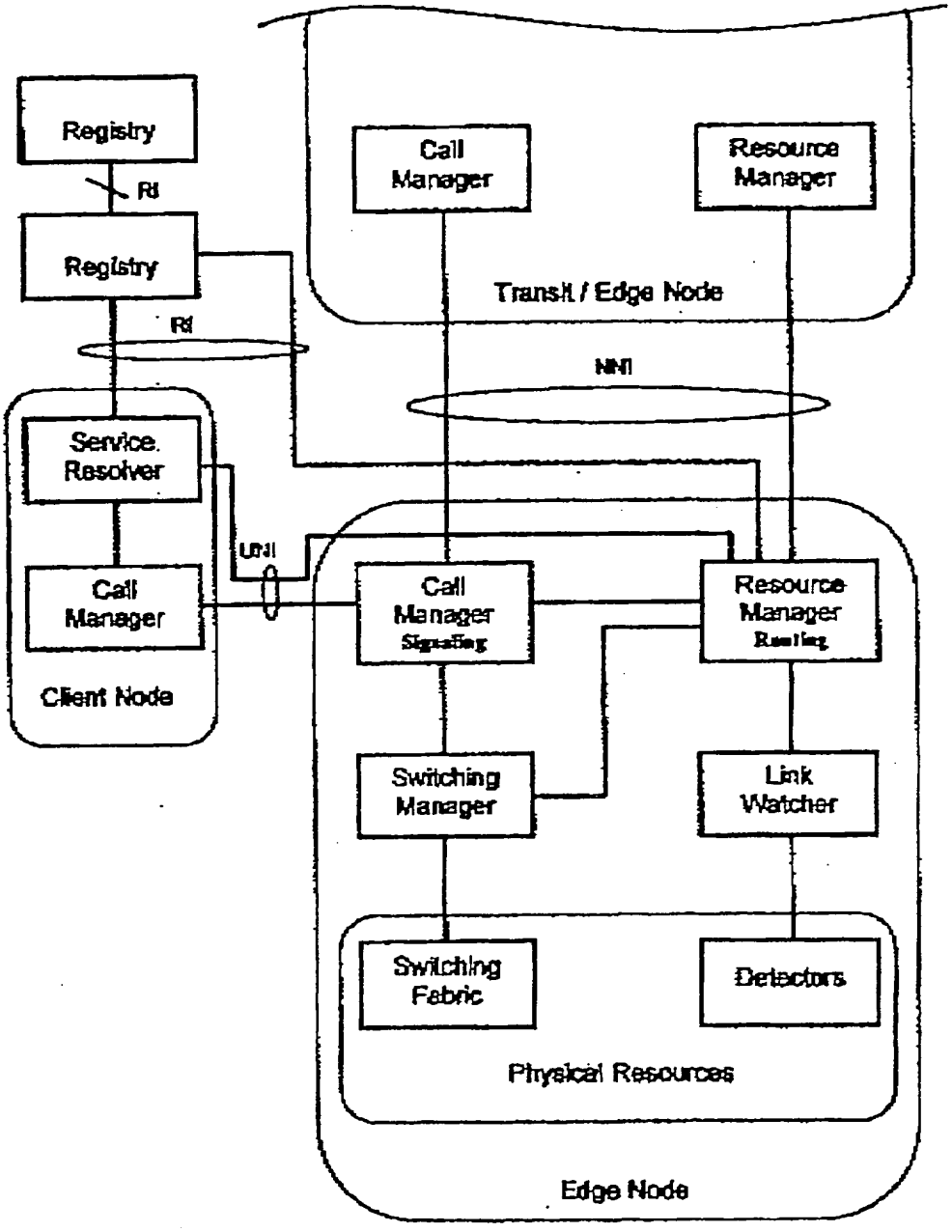

Figure 5-1: ASON functional entities overview

5.2 Switching Fabric

The switching fabric is composed of a space-switching unit and an optional frequency-switching unit (wavelength converters). The switching fabric supports only point-to-point connections. That means the fabric can only connect a single unused output port to a single unused input port. Under the assumption that WDM multiplexers are connected to the switching fabric every port is assigned to a specific wavelength. If the optional frequency-switch is not available the switching fabric can only connect output port to an input port if the assigned wavelengths of both ports are identical. This limitation does not exist for ports with an additional wavelength converter. In this case any unused output port can be connected to any unused input port.

The degree of transparency of the switching fabric must fit the network the fabric belongs to. A transparent switching fabric is universally applicable and can be applied in every network (fiber, transparent, 2.5 Gbit/s etc.). An opaque fabric is almost as flexible applicable as a transparent fabric except to fiber switched networks because complete WDM-signals cannot be switched. A protocol and bit rate specific space switch is limited to networks matching exactly the protocol and the bit rate of the fabric.

5.3 Switching Manager

The switching manager configures the switching fabric and provides an interface for the call manager to set-up and tear-down a connection. The resource manager can directly request the switching state from the switching manager over an additional interface. This allows the resource manager to rebuild its database after reboot of the node.

In network elements which are not fully equipped with wavelength converters a connection set-up may block. Blocking occurs if the wavelength assigned to the input and the wavelength assigned to the output port are not identical and no wavelength converter is available for that connection. In this situation the switching manager rejects the set-up request.

5.4 Call Manager

The call manager runs the signaling protocol for the UNI and NNI to set-up, tear-down and modify end-to-end paths. Such a path has the following attributes:

- Endpoint address
- Signal type
- Protection/working path (in case of a protection path the path ID of the working path)
- Restoration
- Stiffness
- Route (for explicit routing)

Set-up:
Set-up a point-to-point optical path between two network elements.

Tear-down:
Tears-down an established optical path.

Modify:
Modifies an attribute (stiffness, route, restoration properties) of an already established optical path.

An optical path is characterized by the following attributes:

Endpoint address:
An unique address associated with each endpoint of an optical path guarantees a clear identification (see section 4).

Signal type:
Specifies the type of the client signal to be transported over the optical path. The facilities along the optical path, including links, nodes and endpoints must support the requested type. In this context support does not mean that each node must be able to terminate the requested signal type. Termination is necessary at the endpoints of the optical path, but not in between. There it is sufficient that the node is able to switch the client signal. An example of a signal type is STM-16.

Protection/working path:
Specifies whether the optical path is a protection path or a working path. If it is a protection path additional attributes specify the path ID of the associated working path and the diversity (link or node).

Restoration:
Specifies whether the optical path is rerouted in case of a failure.

Stiffness:
Stiff connections, once established, remain until they are released. In contrast, flexible connections may be rerouted during service to allow for network optimization. (See also section 2.1.)

Route:
Specifies the route to set-up an explicitly routed optical path.

The necessary resource and routing information to perform set-up, tear-down and modify actions is requested from the resource manager as needed. For a path set-up the call manager requests the next hop from the resource manager. The information about the next hop provided by the resource manager contains the entire address except the wavelength. The wavelength assignment is done by the call manager during the set-up procedure.

The call manager communicates to adjacent call managers over a bi-directional control channel to exchange signaling information. The knowledge about adjacent call managers is either the result of a configuration process or of an automatic discovery process. An in-band control channel enables the call manager to automatically discover adjacent call managers by sending a hello message. If the control channel is out-band an automatic discovery is not possible but the adjacent call managers have to be configured manually in the database of each call manager. The benefit of getting the information about adjacent call managers from a own database located in the call manager itself is a higher degree of autonomy of the signaling process. Hence it is guaranteed that in case of explicit routing the call manager can handle the entire set-up, tear-down and modify procedures without the help of the resource manager (routing protocol).

5.5 Resource Manager

The resource manager keeps track of the network's resources state. The network resources are represented by the topology consisting of nodes and links. Any pair of nodes in the topology

may be connected by no, one or multiple links. Channel related information (TDM or WDM) is not contained in the topology. The resource manager stores the information about the link resources and the resource attributes. The available (i.e. unused) link resources may also be stored. The resource manager does route computation based on the topology and the resource information, and stores the information of routed paths.

The instantiation can be done as one instance per node. It may be also possible to perform one central (possibly backed-up) instance per domain or several instances per domain. This, however, is not considered in this document.

The resource manager gets the link information from the link watcher, in order to update the stored topology. Upon link connection the entry for the link is allocated in the resource database.

The resource manager provides the call manager with route information consisting of a sequence of nodes including (if needed) the intermediate links. The resource manager gets the information about allocated or de-allocated resources from the call manager to update the stored routing database.

The resource manager provides the registry with the address information of allocated nodes (via the RI). Resource managers update resource information among each other (via the NNI).

Route computation is done based on the topology and the resource state, and subject to client signal parameters (e.g. protection requirements) and physical constraints.

Flexible connections may be rerouted to assure efficient resource utilization. Rerouting may be initiated by the operator or in consequence of a resource manager's route computation. In the latter case the resource manager then initiates the rerouting of affected flexible connections at the call manager.

At start-up the resource manager aligns its database by requesting information from the switching manager, other resource managers and the link watcher.

Basic requirements are that the resource database has to be consistent and that the messaging is reliable.

In current protocols the resource manager function is realized e.g. by the Flooding Protocol and the Exchange Protocol in OSPF or by the Flooding Protocol in IS-IS.

Note: A detailed listing of managed resources is out of the scope of this document.

5.6 Link Watcher

The task of the link watcher is threefold. Firstly, the link watcher detects neighbor nodes. Secondly, the link watcher provides the resource manager with the link attributes. Thirdly, the link watcher notifies the resource manager about link disconnection.

The instantiation can be done as one single instance per node or as one instance per port.

The link watcher interfaces the detectors for link up/down indications, signal performance indications, etc. The link watcher provides the resource manager with the link attributes (link type, shared risk group, etc.)

Reliable messaging is a basic requirement.

5.7 Registry

The registry provides information about reachable client nodes and returns the destination address.

The instantiation can be done as one centralized (possibly backed-up) instance per domain, as several instances per domain or as one instance per node. For each of these cases either a flat realization is possible, or a hierarchy resulting in multiple instances.

In the case of multiple registry instances, the registries request reachability and address information among each other (via the RI). The registry provides the information about the reachability and the address of a node requested by the service resolver (via the RI).

Requirements are that the database has to be consistent and that the messaging is reliable.

The registry function can be compared with the Non-Broadcast, Multi-Access (NBMA) Address Resolution Protocol (NARP). If the network consists of multiple subnetworks, the comparison with the NBMA Next Hop Resolution Protocol (NHRP) holds. NHRP is a functional superset of NARP to provide addresses of "nearest" egress nodes for destinations outside the subnetwork.

5.8 Service Resolver

The service resolver queries the registry before initiating the call.

The instantiation is performed at clients (with UNI).

The service resolver queries the registry for a destination node's address (via the RI). If the node is reachable the service resolver initiates the call at the client node's call manager. Otherwise the service is rejected as unresolvable.

A basic requirement is reliable messaging.

6 OPERATIONAL DESCRIPTION

6.1 Information Flows between Functional Entities

6.1.1 Network Augmentation: Adding a new Node

If a new network node is added, its link watcher checks if the node is physically linked to its neighbors (by means of the detectors for link up/down indications).

A new network node, going on-line, has to exchange database information of the resource manager with its neighbors. (All information about the node's resources and their current use is concentrated in the resource managers database.)

For that, the new node's resource manager first listens to "Hello" messages, discovers these neighbors and then sends out its own "Hello" messages to let the neighbors know that it is active. Next, the resource manager database information is exchanged with adjacent network nodes (in OSPF with so-called "Database Description" and "Link State Request" / "-Update" messages).

Data to be exchanged are: link attributes (node address and attributes, link type, shared risk group, etc.) and link resource information (fibers, wavelengths, bandwidth, etc.)

After that the new node's call manager is able to establish the working and protection paths using the network topology information stored in the resource managers database.

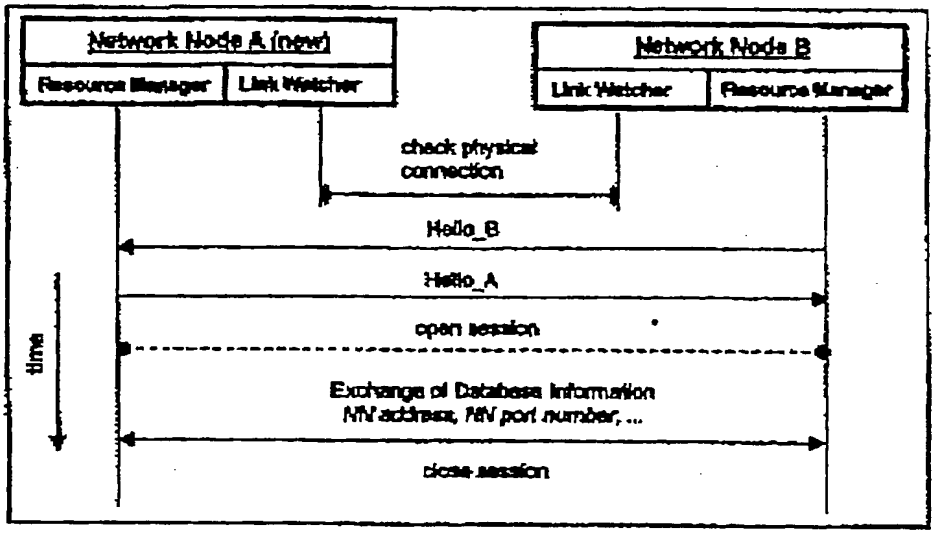

Figure 6-1: Event sequence for adding a new node

6.1.2 Network Augmentation: Adding a new Client

To be "reachable" by other clients, a new client advertises itself to the registry. (Alternatively, it could be done by the resource manager of the network node the client is attached to.) Information to be delivered to the registry is:

1. the client network address
2. the network node address the client is connected to
3. the port number of the network node
4. the interface type

(It is assumed that the client is connected via a transponder. Otherwise, the used wavelength also has to be stored.)

An active network node periodically broadcasts "Hello" messages ("I am active", not necessarily identical with OSPF's "HELLO" messages, distributed between the network nodes) to all its potential client interfaces.

After connecting a new client to the network node, it receives the network node's "Hello" message ("Hello_NN") and starts sending its own "Hello" messages ("Hello_C") to the network node (sequence can be inverted). A session is established between the two, more precisely between the client's service resolver and the network node's resource manager. So the client gets the node's address information needed for advertising to the registry: node address, port number and the registry address (if RI is not a separate physical interface).

Then the client advertises to the registry via the RI interface. After successful advertisement the service resolver enables the call handling.

In case of a dead network node no "Hello_NN" message is received and the client informs the registry to be set to "non reachable".

If an active client becomes unreachable (because the client crashes or the connection to the network node is broken) the network node does not get "Hello_C" and its resource manager sends a message to the registry to cancel the client from the database.

Then, after reboot and/or receiving "Hello_NN" message from the network node the whole prodedure described above is executed again.

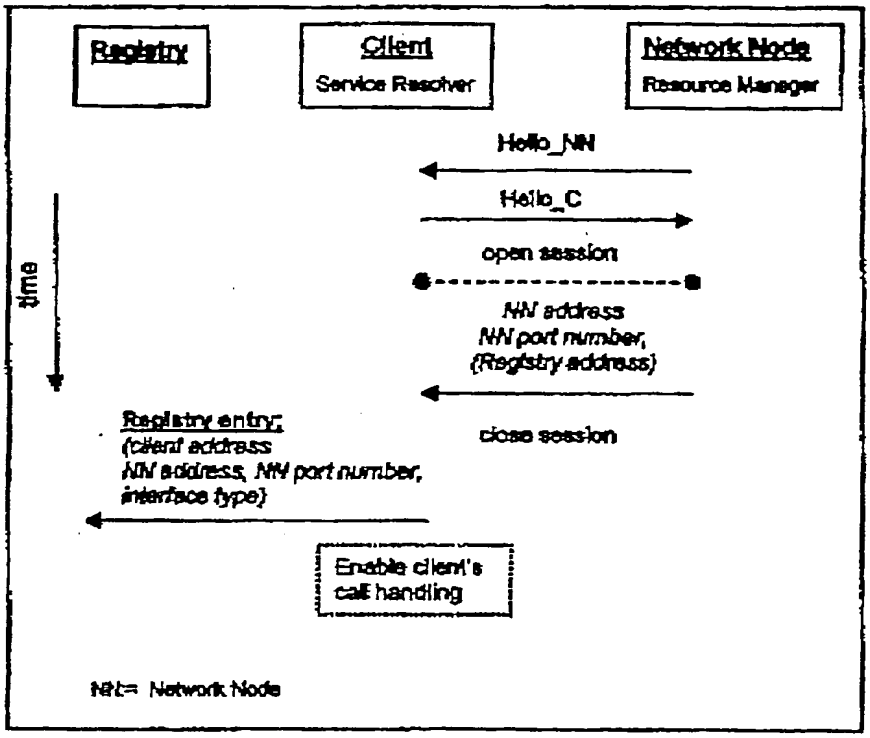

Figure 6-2: Event sequence for the addition of a new client

6.1.3 State Information Update

State information may be updated even in absence of topology changes or call actions. The resource managers periodically check the consistency of the (distributed) databases, and synchronize these if needed. Available link resources, which may not be advertised so often, can be updated by this.

Distributed route computation is commonly done using routing weights. The routing weights or the calculation of these weights (e.g. if these are a function of the available resources) may be changed during the network operation, e.g. for traffic engineering purposes.

For synchronization the aging mechanism of OSPF can be employed [8]. By associating an age for database records, the entries can be updated automatically.

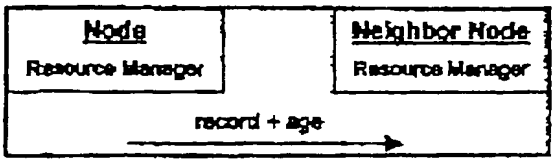

Figure 6-3: State information update

6.1.4 Basic Call: Set-up

This section describes the set-up of a bi-directional point-to-point (working) path between two network elements. At first we consider a flat wavelength routing network without any multiplexing hierarchy. Further we assume that for every optical path an associated path in the other direction exists. That means all network resources like wavelengths, links, ports, etc. only exist in pairs, one for the down-link and one for the up-link. Thus, the routing and wavelength assignment have to be solved just once for a bi-directional path.

The network elements may be equipped with wavelength converters or not. Hence, the wavelength assignment has to be solved in general for an optical path covering network elements with and without wavelength converters. However, all clients are connected via tunable transponders which are able to convert any input wavelength to any desired output wavelength. This guarantees that over the UNI no wavelength availability information has to be exchanged and that the choice of a proper wavelength is completely independent of the clients wavelength. The set-up procedure is based on an AT&T proposal [6] and is extended to meet our requirements. The procedure is now described with the help of Figure 6-4.

Client 1, an IP router connected to an optical network wants to establish a shortcut to client 2, another IP router which is connected to the optical network as well. Firstly, client 1 needs to know if client 2 is reachable through the optical network and if so client 1 needs to know the address of client 2. The service resolver of client 1 requests the reachability and address information of client 2 from the registry over the RI interface. If client 2 is reachable the service resolver initiates the path set-up with the desired attributes (endpoint address, path type, protection, etc.) at the call manager. Then the client call manager sends a path set-up message with the associated attributes over the UNI to the call manager of the optical node A. To allow a clear identification of a specific optical path, node A (ingress) chooses a unique label as a path identifier. During the path set-up the path identifier is transmitted to every node along the route and to both clients. The path identifier is saved in every node along the route as long as the associated optical path exists.

To establish an optical path from node A to node E a wavelength request message is sent from the call manager in node A to the call manager in the next hop node B. The next hop is provided by the resource manager on a request of the call manager (hop-by-hop routing). The wavelength request message which is sent downstream contains a path vector which informs the following nodes about the nodes already covered by the path and the available wavelengths (a vector of the same size as the number of wavelengths on the first link). The first wavelength request message along the route contains therefore just a single entry "A 10000011". This message informs node B that the wavelengths 1,7 and 8 are available on link AB. In the example an 8 channel system is assumed. Because node B does not contain a wavelength converter the wavelength must continue. This can be guaranteed by canceling all wavelengths in the received wavelength availability vector which are not available on link BC. In the example the wavelengths 7 and 8 have to be canceled. The wavelength request message now contains two entries and is sent to the next hop C. In node C a wavelength converter is available. Hence,

the necessity for wavelength continuity does not exist and all available wavelengths on link CD can be used. Thus, a new entry "C 00111000" is added to the path vector and the wavelength request message is sent to the next hop D. As soon as the end node E is reached a wavelength allocation message is sent back to the beginning of the path along the route specified by the path vector. The wavelength assignment can now be done by every node. For selecting a proper wavelength the path and wavelength availability vector received together with the wavelength request message is temporarily stored by each node as long as the wavelength allocation is finished. In the example the first fit algorithm is applied for the wavelength assignment. But the procedure is not limited to the first fit algorithm, other wavelength assignment algorithms can be applied as well.

The availability of all the wavelengths marked in the path vector as available must be guaranteed as long as the wavelength allocation message has been received. After allocating a proper wavelength the unused but reserved wavelengths can be released. Reserving all wavelengths along the route for the entire set-up process does not allow the simultaneous set-up of more than one path if the routes have coincidence links. This can dramatically increase the time necessary for setting up restoration calls after a failure. To allow the simultaneous set-up of more than one path the wavelengths could be divided into groups. After selecting a wavelength group the edge node A sends a wavelength request message with the group ID and the wavelength availability vector for that group along the route. Now the reservation is only necessary for one group. Unused wavelength outside this group can be used to set-up additional paths simultaneously. Work on this topic is still in progress.

If the bandwidth resources on a link along the route from A to E are exhausted, a reject message is sent back to the transit node A and all reserved wavelengths along the route have to be released. That means that the requested optical path cannot be established. To achieve better network utilization alternate routing or crank back can be implemented.

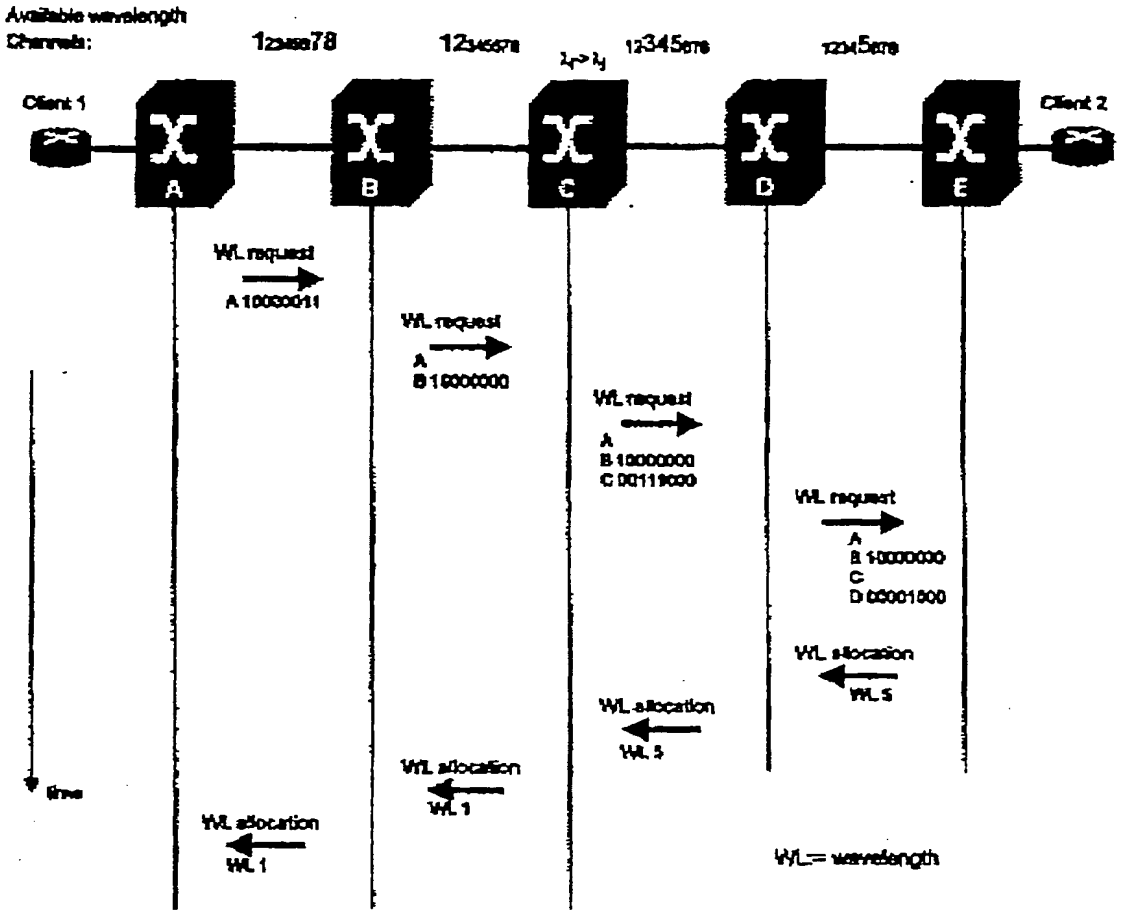

Figure 6-4: Optical path set-up

In a hierarchical network with multiplexers the call set-up may take place over several multiplex layers (see Figure 2-1). The call set-up for the TDM layers is slightly different to the above described set-up in the wavelength routing layer. For the TDM layers no equivalent to the wavelength continuing constraint exists. That means the channels can be switched from one time slot to any other available time slot. This is equivalent to a wavelength routing layer every node fully equipped with wavelength converters. Hence, in the TDM layers the transmission of a channel availability vector equivalent to the wavelength availability vector in the wavelength routing layer is not necessary.

6.1.5 Protected Call: Set-up

To protect the optical path from A to E against failures the client may set-up an additional path (protection path) on a diverse route. In case of a failure both client nodes switch from the working path to the protection path. To set-up a protection path on a diverse route the route of the working path must be known. Node A gets this information in form of a working path ID from the client requesting the protection path. Node A initiates now the protection path set-up by sending a new wavelength request message to the next hop of the protection path. The request message contains the working path ID to avoid coincidence of nodes or links between working

and protection path. The set-up procedure is almost the same as for the working path but with an additional constraint for the routing algorithm to avoid nodes which are part of the working path.

6.1.6 Call tear-down

Assumed the optical path (working or protection) from client 1 to client 2 we have set-up in section 6.1.4 should be torn down. The path tear-down can be triggered from both sides, either from client 1 or from client 2. For the following description we assume that client 1 triggers the path tear-down. The service resolver initiates the path tear-down of the desired path (attributes: endpoint address, path type, etc.) at its call manager. Then the call manager sends a path release message with the associated attributes over the UNI to the call manager of the optical node A. A wavelength release message is sent along the path from node to node until the edge node E is reached. As soon as the call manager in the edge node receives the release message it informs the call manager of client 2 that the optical path is about to be closed. After client 2 has agreed or a time out has expired the call manager in the edge node sends a wavelength release message back to node A. Every node along the path that receives this wavelength release message releases all resources associated with the path to be closed.

The described procedure for the path tear-down can be applied in hierarchical networks (with TDM multiplexers) as well.

6.1.7 Restoration Call

As an option, the ASON can restore connections which are not protected by back-up connections.

The restoration attribute for a connection is signaled via the UNI. The corresponding edge node tags the connection as restorable and is responsible for the restoration.

There are two possibilities to trigger a restoration call:

Triggered by link watcher:

> The link watcher detects the failure of the link (e.g. by the failure of the link's in-band control signal) and indicates this to the resource manager.
>
> The resource manager identifies in the database all the connections over the failed link and initiates release messages for each connection. An edge node receiving a release message for a tagged connection then initiates the restoration call for this connection.

Triggered by transponder:

> The transponder at the end of the connection detects that the signal does not meet the desired quality (e.g. through performance monitoring or detecting a Loss of Signal) and then indicates this to the resource manager of the edge node.
>
> If the connection is tagged, the connection will be released and restored by the edge node.

As a link watcher-triggered example, Figure 6-5 depicts the situation for a uni-directional failure between B←C on the (bi-directional) path A-B-C-D requested by client 1. The link watcher at B detects the failure. By net_release messages from B for both ends of the path the connection is released and the edge node A restores the connection by rerouting over A-B-E-...-D.

In case of a bi-directional failure both B and C send net_release messages to the edge nodes. This is analogous to a node failure on the path, e.g. for a further node between B and C.

If one of the edge nodes failed, restoration is not possible anymore. If the edge node of the requesting client failed, then that path cannot be restored anymore. The client may be notified about the failure of the node. If the edge node of the destination client failed, the set-up(s) of the restoration path(s) will fail. At the end of the trial(s) the client will be notified about the unsuccessful restoration call.

In the example, a transponder-triggered restoration will behave analogous, except that the release messages are initiated by the edge node.

In principle one or both of the trigger possibilities may be employed. In the latter case, possible interactions have to be considered. E.g. the edge nodes may incorporate some hold-off time in the transponder-triggered restoration.

The edge node may perform some prioritizing of simultaneous restoration calls, e.g. stiff connections before flexible connections, since flexible connections can be optimized later on.

For a new (restored) connection, edge nodes may select new wavelengths for the transponders. If the restoration call failed, the clients at both ends will be will be notified over the UNI.

For the path restoration, advanced rerouting mechanisms may be employed. E.g. a new route may be established by using loose explicit routing and taking the actual failure state into account. Also the edge node may employ some set-up re-trial mechanisms.

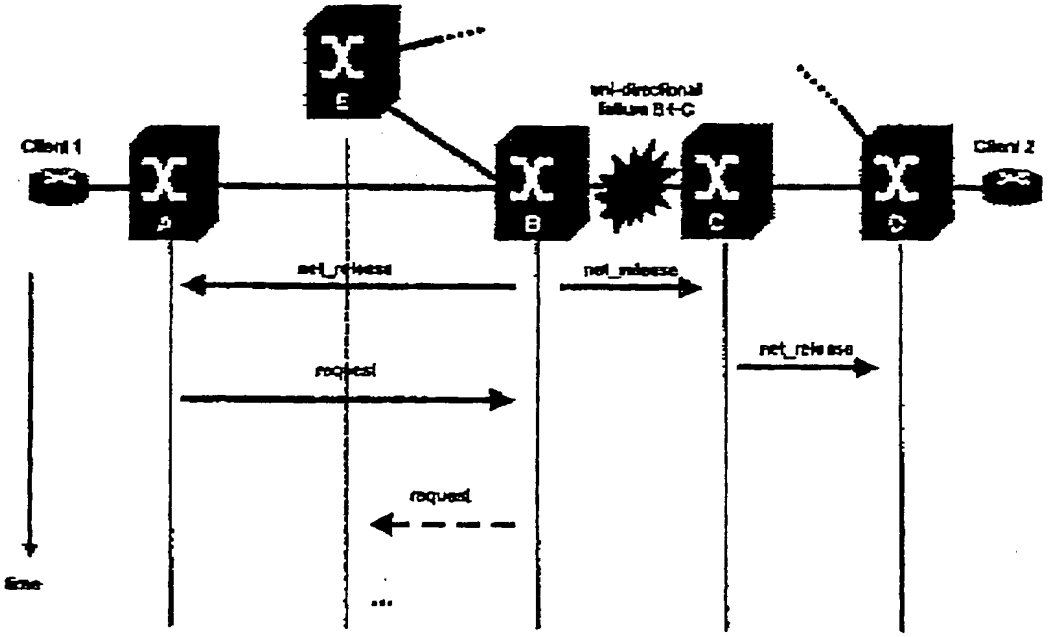

Figure 6-5: Restoration of an optical path

6.1.8 Modify Call

The modify call is triggered by an operator via a network management system to reroute an already existing optical path. The rerouting of an optical path can be desirable to optimize the network or to lockout traffic from a specific link (e.g. for maintenance). A modify call routes a new path through the network and switches the traffic from the old path (the path to be

modified) to the new path as far as the resources for the new path have been reserved. Establishing the new path before breaking the old one guarantees short switching times and the availability of the new path under all circumstances. If the call set-up of the new path blocks, the old path remains established.

A special feature of a modify call is the possibility that the new path may use the same resources than the old one. In Figure 6-6 for example, the modify call is allowed to use the same wavelength on link AB as the old path. For this reason the path ID of the old path is sent together with a wavelength (WL) request message during the set-up of the modified call. A wavelength which is used by the old path is marked in the wavelength availability vector as unused. This guarantees that all resources used by the old path are also available for the new one. After the wavelengths along the route of the new path are allocated and the connections in the switching fabrics are established, the old path can be closed. The tear-down procedure of the old path needs to know the path ID of the new path to avoid the release of resources used by the new path as well.

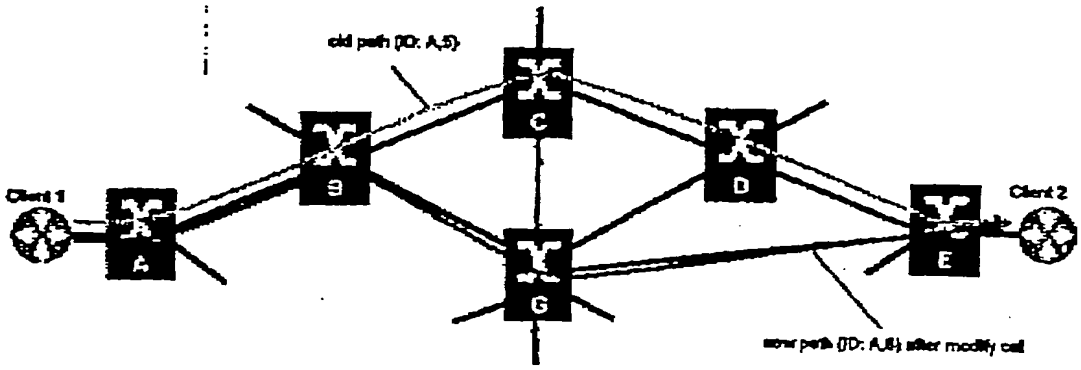

Figure 6-6: Modify call

6.2 Routing in Hierarchical Networks

In Section 2.3 the hierarchical layering of the ASON due to TDM has been described. Below a method is introduced which allows to route a path through such a network.

For the following description the terminology of G.805 will be employed [7]. Additionally, the term interchange node is used, denoting a node with access to link connections which are realized by a trail of another ASON layer network. Only those layer networks comprising matrix connection functions are of relevance for the routing algorithm and are therefore meant, if the term layer network is used within this context. Keeping this in mind, an interchange node may also be described as a node with at least one junction to another layer network which is acting as a server layer for it. Note, that the respective node in the server layer may not be an interchange node.

Each layer network has its own routing instances. In Figure 2-1 for instance, there are three sets of routing instances forming three peer groups. A node belonging to two layer networks runs therefore two independent routing instances.

The topology of a layer network comprises the nodes (interchange and ordinary nodes) and the links between them. Individual link connections are not part of the topology. If there are link connections between two interchange nodes which are realized by a server trail, a

representative, reflecting this server trail, is part of the client layer topology, see Figure 6-7. There the topology of the client layer network comprises two interchange nodes, an ordinary node, two links, and a representative. The representative is only a reminder, that there is the possibility to establish a connection between the respective interchange nodes. If at least one link connection is actually used, a link parallel to the representative is included in the topology. This link may now act as a server trail for another layer network resulting in a representative in the respective layer. If all link connections supported by a server trail are occupied, the representative is deleted from the topology but not the link parallel to it.

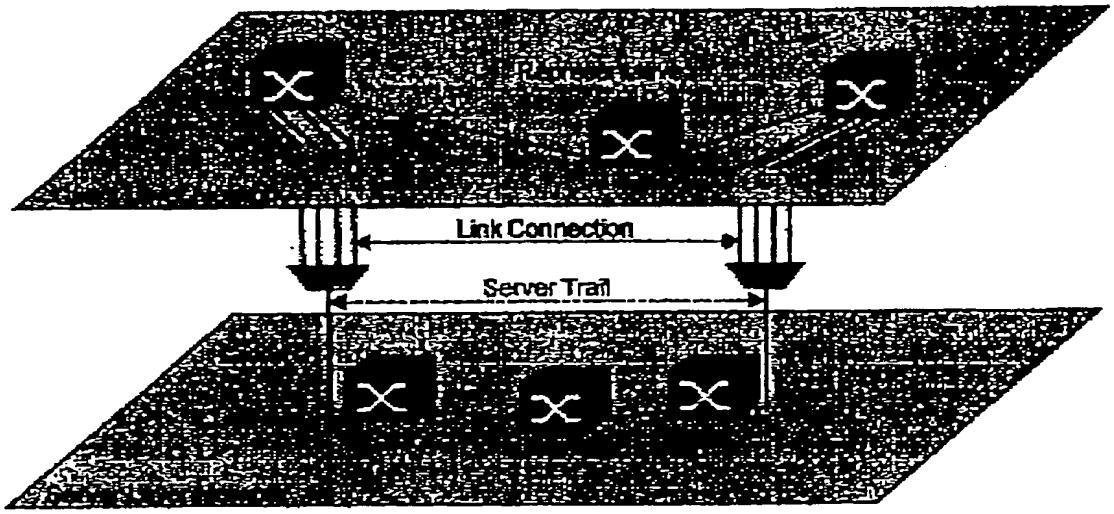

Figure 6-7: Representing a server trail in the client network

An example will help to clarify the procedure. Assume that there is a 2.5 Gbit/s network above a 10 Gbit/s network above a 40 Gbit/s network. An established 40 Gbit/s server trail will be reflected in the 10 Gbit/s network by a representative. This representative reminds the routing instances running in the 10 Gbit/s layer that there is capacity for the transport of 10 Gbit/s signals between the two interchange nodes terminating it. Up to now the 2.5 Gbit/s layer is not aware of the possibility to use part of the capacity of this 40 Gbit/s trail. This changes in case one of the four 40 Gbit/s tributaries is actually used by the 10 Gbit/s network. Now parallel to the representative a link is included in the 10 Gbit/s layer, and this link causes a representative to be included in the 2.5 Gbit/s layer, given the required multiplexers are installed (the respective 2.5 Gbit/s nodes are interchange nodes). A 2.5 Gbit/s link connection may now be used which is carried by a 10 Gbit/s trail which is running over a 40 Gbit/s trail. If all link connections supported by one server trail are already used, there is no need for a representative as a reminder for potential link connections and therefore it is deleted. However, the link cannot be deleted because part of its capacity may still be available, e.g. a 2.5 Gbit/s time slot in a 10 Gbit/s signal may still be free while all four 10 Gbit/s tributaries of the 40 Gbit/s signal are used.

It should be noted, that in the ASON a client layer may comprise representatives of different server layers, e.g. a 2.5 Gbit/s layer network may have representatives due to a 10 Gbit/s server layer as well as due to a 40 Gbit/s server layer if the latter provides directly 2.5 Gbit/s tributaries. Also the transparent network layer may have representatives in all other layer networks, see Figure 2-1.